UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/357,483	07/20/1999	STEPHEN MICHAEL MATYAS JR.	5577-170	9314

20792 7590 05/21/2004

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	11

DATE MAILED: 05/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/357,483	MATYAS ET AL.	
	Examiner	Art Unit	
	Paula W Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) *1-16,22,23,25,26,28-39 and 43-54* is/are allowed.

6)☒ Claim(s) *17-19,24,27,41-40, 55-56* is/are rejected.

7)☒ Claim(s) *20,21,42,and 57* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 2/20/04 (Paper No. 10). The amendment filed on 2/20/04 have been entered and made of record. Therefore, presently pending claims are 1-57.

Response to Arguments

Applicant's arguments filed 2/20/04 have been fully considered but they are not persuasive because of following reasons given below.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner asserts that Rivest and Matya does teach or suggest the subject matter broadly recited in independent Claims 17, 24, and 27. Accordingly, rejections for claims 17, 24, and 27 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 17-19, 24, 27, 40-41, and 55-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matya (6,687,375 B1) in view of Rivest et al.

In reference to claims 17, 24, and 27, Matyas discloses a method of generating a cryptographic key utilizing user specific information. Recovering W`p form the first and second candidate cryptographic value p` and publicly known seed value IV (publicly know biometric).

Using a function f and a random number corresponding to p. The seed value that is generated is put through a PRNG to generate p`` which would utilize $W`_p$ and IV, since values are used to calculate the seed value for the PRNG, the seed is dependent on $W'_p$ and IV. The same would be repeated for q`` (column 9 line 45-67). Matyas also discloses performing a biometric verification using the procedure for generating the key as shown above and comparing it with a stored value (column 15 lines 9-26).

Matyas does not disclose finding p and q from N and d.

However, Rivest discloses a method of recovering the cryptographic values p and q by factoring n since it can be done easily once d is known (page 12 section C paragraph 2). The comparison is then an elementary mathematic computation. It is well known that an authentication process includes generating keys that are compared to the expected keys.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to find p and q as disclosed by Rivest and use the values of p and q to perform the biometric validation as in Matyas. One of ordinary skill in the art would have been motivated to do this because once N and d are known it is an elementary procedure to calculate p and q and therefore the system would save memory by calculating them.

In reference to claims 18, 40 and 55, the step of determining that the RSA cryptographic values are not authentic if p` and q` are values outside the user defined segments of the first and second intervals (column 10 lines 35-51). The original secret seed and biometric would be required to find the p and q and therefore they are not authentic if they are not equal to p and q which would correspond to falling in the segments of p and q.

In reference to claims 19,41, and 56, the size of the cryptographic values would depend on the selection of the seed.

Allowable Subject Matter

The following is a statement of reasons for the indication of allowable subject matter:

Independent claims 1, 22, and 25 are allowed. Matyas discloses finding RSA cryptographic values p and q from biometric. Rivest discloses using the values in the RSA encryption. Matyas and Rivest do not disclose searching for the values of p and q from the biometric segments that are mapped to the intervals of the possible RSA values.

Dependent claims 2-16, 23, 26, 28-39,and 43-54 are allowable because they are dependent on allowable claims.

Claims 20-21, 42, and 57 are objected because they are dependent on rejected claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, May 17, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 21[illegible]